CLAIMS

We claim:

1. An apparatus for key management comprising:

(a) a multitude of key registers, said multitude of key registers having a hierarchy with levels;

(b) a multitude of type fields, wherein each type field is associated with a key register;

(c) a key management controller, said key management controller having a multitude of modes;

(d) at least one initialization vector;

(e) key management algorithms; and

(f) key management functions;

wherein said mode is determined by the hierarchical level of the key register, and the key management algorithm used is determined by the key management function being used and said mode.

2. The apparatus according to claim 1 wherein said multitude of modes includes a CBC' mode.

3. The apparatus according to claim 2 wherein said multitude of modes further includes a CBC mode.

4. The apparatus according to claim 2 wherein said multitude of modes further includes an ECB mode.

5. The apparatus according to claim 4 wherein said ECB mode uses a deterministic non-identity function.

6. The apparatus according to claim 4 wherein said ECB mode uses swapped key blocks.

7. The apparatus according to claim 3 wherein said CBC mode uses a firmware specified initialization vector.

8. The apparatus according to claim 2 wherein said CBC' mode uses an initialization vector to wrap level i red key bits, said initialization vector determined by level i.

9. The apparatus according to claim 2 wherein said CBC' mode uses an initialization vector to unwrap black bits to level j, said initialization vector determined by level j.

10. The apparatus according to claim 4 wherein at level 0 said mode is ECB mode and said multitude of functions include:

(a) an encode function; and

(b) a decode function.

11. The apparatus according to claim 4 wherein at level 1 said multitude of functions includes:

(a) an unwrap black bits to level 0 function, wherein said mode is a CBC mode with a firmware specified initialization vector; and

(b) an encode data function, wherein said mode is an ECB mode using a swapped key blocks.

12. The apparatus according to claim 4 wherein at level 2 said multitude of functions includes:

(a) a wrap level i red key bits, wherein said mode is a CBC' mode with an initialization vector determined by the level i;

(b) an export black bits function;

(c) an unwrap black bits to level j as determined by firmware, wherein said mode is CBC' mode with an initialization vector determined by the level j; and

(d) an import red key bits as level 0 function.

13. A method for generating an encoded value having a first encoded value part and a second encoded value part from an unencoded value having a first unencoded value part and a second unencoded value part, comprising the steps of:

(a) obtaining an initialization vector;

(b) generating the first encoded value part by:

(i) generating a first result by encrypting the first unencoded value part;

(ii) generating a second result by performing an exclusive or operation on the first result and the second unencoded value part;

(iii) generating a third result by performing an exclusive or operation on the second result and the initialization vector;

(iv) generating a fourth result by encrypting the third result;

(v) generating a fifth result by performing an exclusive or operation on the fourth result and the first unencoded value part; and

(vi) encrypting the fifth result; and

(c) generating the second encoded value part by encrypting the second result.

14. A method according to claim 13, wherein said step of obtaining an initialization vector further includes the steps of:

(a) determining a hierarchical level for the encoded value; and

(b) obtaining the initialization vector determined by the hierarchical level.

15. A method for generating an unencoded value having a first unencoded value part and a second unencoded value part from an encoded value having a first encoded value part and a second encoded value part, comprising the steps of:

(a) obtaining an initialization vector;

(b) generating the first unencoded value part by:

(i) generating a first result by decrypting the second encoded value part;

(ii) generating a second result by performing an exclusive or operation on the first result and the initialization vector;

(iii) generating a third result by encrypting the second result;

(iv) generating a fourth result by decrypting the second encoded value part; and

(v) performing an exclusive or operation on the third result and the fourth result;

(c) generating the second unencoded value part by:

(i) generating a fifth result by encrypting the first unencoded value part; and

(ii) generating a sixth result by decrypting the second encoded value part; and

(d) performing an exclusive or operation on the fifth result and the sixth result.

16. A method according to claim 15, wherein said step of obtaining an initialization vector further includes the steps of:

(a) determining a hierarchical level for the encoded value; and

(b) obtaining the initialization vector determined by the hierarchical level.